

IN THE CLAIMS

Please amend the claims as indicated:

1. (currently amended) A method for managing a network boot of a client computer, the method comprising:

storing a list of trusted Pre-boot eXecution Environment (PXE) boot program servers in an interface service card coupled to a client computer on a network, the interface service card also being coupled to a hyper-secure remote service network that includes a remote supervisor computer, wherein the remote supervisor computer controls the storage of the list of trusted PXE boot program servers in the interface service card;

broadcasting a request for a boot program from the client computer to a network of PXE boot program servers;

receiving a response to the request for the boot program at the client computer, the response being from a responding boot program server on the network of PXE boot program servers;

comparing an identity of the responding boot program server with the list of PXE trusted boot program servers; and

upon verifying that the responding boot program server is on the list of PXE trusted boot program servers, requesting and downloading onto the client computer a boot program from the responding PXE boot program server.

2. (currently amended) The method of claim 1, further comprising:

[[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, blocking the requesting of the boot program from the responding boot program server.

3. (currently amended) The method of claim 2, further comprising:

[[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, generating an alert to a designated administrator of a presence of an unauthorized boot program server on the network of boot program servers.

4. (cancelled)

5. (currently amended) The method of claim [[4]] 1, wherein the comparing step is performed by configuring the client computer to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI) model.

6. (currently amended) The method of claim 1, further comprising:

[[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, downloading a boot program from a known trusted boot server in a secure local area network (LAN).

7. (original) The method of claim 1, wherein the client computer is a server blade.

8. (original) The method of claim 7, further comprising:

managing different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade, a permission list of boot program servers authorized for each server blade in a server blade chassis.

9. (currently amended) A system for managing a network boot of a client computer, the system comprising:

means for storing a list of trusted Pre-boot eXecution Environment (PXE) boot program servers in an interface service card coupled to a client computer on a network, the interface service card also being coupled to a hyper-secure remote service network that includes a remote supervisor computer, wherein the remote supervisor computer controls the storage of the list of trusted PXE boot program servers in the interface service card;

means for broadcasting a request for a boot program from the client computer to a network of PXE boot program servers;

means for receiving a response to the request for the boot program at the client computer, the response being from a responding boot program server on the network of PXE boot program servers;

means for comparing an identity of the responding boot program server with the list of PXE trusted boot program servers; and

means for, upon verifying that the responding boot program server is on the list of PXE trusted boot program servers, requesting and downloading onto the client computer a boot program from the responding PXE boot program server.

10. (currently amended) The system of claim 9, further comprising:

means for, [[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, blocking the requesting of the boot program from the responding boot program server.

11. (currently amended) The system of claim 10, further comprising:

means for, [[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, generating an alert to a designated administrator of a presence of an unauthorized boot program server on the network of boot program servers.

12. (cancelled)

13. (currently amended) The system of claim [[12]] 9, wherein the means for comparing is performed by means for configuring the client computer to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI) model.

14. (currently amended) The system of claim 9, further comprising:

means for, [[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, downloading a boot program from a known trusted boot server in a secure local area network (LAN).

15. (original) The system of claim 9, wherein the client computer is a server blade.

16. (original) The system of claim 15, further comprising:

means for managing different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade, a permission list of boot program servers authorized for each server blade in a server blade chassis.

17. (currently amended) A computer program product, residing on a computer usable medium, for managing a network boot of a client computer, the computer program product comprising:

program code for storing a list of trusted Pre-boot eXecution Environment (PXE) boot program servers in an interface service card coupled to a client computer on a network, the interface service card also being coupled to a hyper-secure remote service network that includes a remote supervisor computer, wherein the remote supervisor computer controls the storage of the list of trusted PXE boot program servers in the interface service card;

program code for broadcasting a request for a boot program from the client computer to a network of PXE boot program servers;

program code for receiving a response to the request for the boot program at the client computer, the response being from a responding boot program server on the network of PXE boot program servers;

program code for comparing an identity of the responding boot program server with the list of PXE trusted boot program servers; and

program code for, upon verifying that the responding boot program server is on the list of PXE trusted boot program servers, requesting and downloading onto the client computer a boot program from the responding PXE boot program server.

18. (currently amended) The computer program product of claim 17, further comprising:

program code for, [[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, blocking the requesting of the boot program from the responding boot program server.

19. (currently amended) The computer program product of claim 18, further comprising:

program code for, [[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, generating an alert to a designated administrator of a presence of an unauthorized boot program server on the network of boot program servers.

20. (cancelled)

21. (currently amended) The computer program product of claim [[20]] 18, wherein the program code for comparing is performed by program code for configuring the client computer to perform Layer 3 packet filtering to identify Pre-boot Execution Environment/Bootstrap Protocol (PXE/BootP) traffic, wherein Layer 3 is a network layer of the seven layers of the Open System Interconnection (OSI) model.

22. (currently amended) The computer program product of claim 17, further comprising:

program code for, [[upon]] in response to determining that the responding boot program server is not on the list of trusted boot program servers, downloading a boot program from a known trusted boot server in a secure local area network (LAN).

23. (original) The computer program product of claim 17, wherein the client computer is a server blade.

24. (original) The computer program product of claim 23, further comprising:

program code for managing different types of boot program servers available to the server blade by maintaining, in an information technology services organization logically oriented between the different types of boot program servers and the server blade, a permission list of boot program servers authorized for each server blade in a server blade chassis.

25. (new) The method of claim 1, wherein the remote supervisor computer is part of an Information Technology (IT) services organization that manages various types of Pre-boot eXecution Environment (PXE) deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer.

26. (new) The system of claim 9, wherein the remote supervisor computer is part of an Information Technology (IT) services organization that manages various types of Pre-boot eXecution Environment (PXE) deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer.

27. (new) The computer program product of claim 17, wherein the remote supervisor computer is part of an Information Technology (IT) services organization that manages various types of Pre-boot eXecution Environment (PXE) deployment servers, and wherein the IT services organization enables a same IT service organization assigned systems administrator to manage the various types of PXE deployment servers, to maintain permission lists for each PXE server type, to monitor a network for a presence of unauthorized PXE servers that are not authorized, by the IT services organization, to support the client computer, and to shut down network ports, for unauthorized PXE servers, in the client computer.